(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2004-318330
(P2004-318330A)
(43)公開日　平成16年11月11日(2004.11.11)

(51)Int.Cl.[7]	F I			テーマコード（参考）
G06F 11/00	G06F	9/06	630A	5B017
G06F 1/00	G06F	12/14	320A	5B076
G06F 9/445	G06F	9/06	640A	
G06F 12/14	G06F	9/06	660L	

審査請求 未請求　請求項の数 11　OL　（全 13 頁）

(21)出願番号　特願2003-109170 (P2003-109170)
(22)出願日　平成15年4月14日 (2003.4.14)

(71)出願人　503121103
株式会社ルネサステクノロジ
東京都千代田区丸の内二丁目４番１号
(74)代理人　100080001
弁理士　筒井　大和
(72)発明者　飯島　雅人
東京都千代田区丸の内二丁目４番１号　株式会社ルネサステクノロジ内
(72)発明者　浅井　俊雄
東京都千代田区丸の内二丁目４番１号　株式会社ルネサステクノロジ内

Fターム(参考)　5B017 AA03　BA04　CA12　CA16
5B076 BB06　EB03

(54)【発明の名称】半導体集積回路装置およびデータ処理システム

(57)【要約】
【課題】外付けで不揮発性メモリが接続可能な半導体集積回路装置において、ユーザデータの書き込み後の該ユーザデータの漏洩を防止する。
【解決手段】リセット後、半導体集積回路装置１がブートモードに遷移すると、ＣＰＵ３がブートＲＯＭ１０からフラッシュメモリ２の制御プログラムをダウンロードするためのブートプログラムを読み出す。続いて、ホストＨとのビットレートの合わせ込みを行い、ＣＰＵ３はフラッシュメモリ２のプロテクトエリアＰＲに書き込まれているプロテクトデータを参照し、該プロテクトデータがプロテクト状態となっているか、否かを判断する。このとき、プロテクトデータがプロテクト状態となっている際には、半導体集積回路装置１は、スタンバイ状態（あるいは、スリープ状態、無限ループ）となり、制御プログラムのダウンロードが一切実行できなくなる。
【選択図】　図２

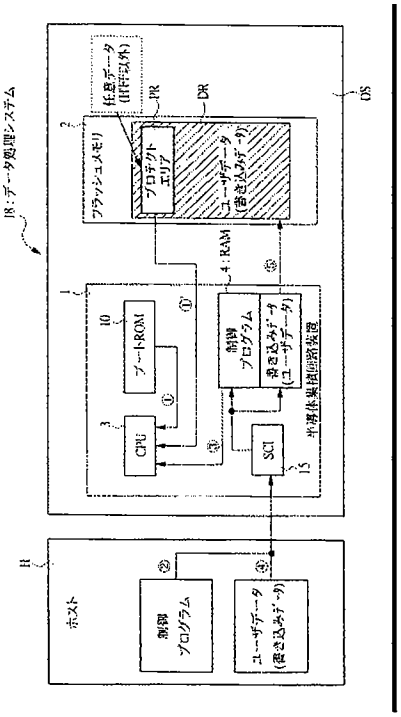


図２

【特許請求の範囲】
【請求項1】
外付けで不揮発性メモリが接続可能で、前記不揮発性メモリを制御する制御プログラムをダウンロードするブートプログラムが格納された半導体集積回路装置であって、
前記ブートプログラムに基づいて、前記制御プログラムをダウンロードする制御部を備え、
前記制御部は、
ブートモードによる起動時において、プロテクトデータに応じて第１、または第２の状態のいずれであるかを判断し、前記第１の状態の際には、前記制御プログラムのダウンロードを実行し、前記第２の状態の際には、前記制御プログラムのダウンロードを実行しないことを特徴とする半導体集積回路装置。
【請求項2】
外付けで不揮発性メモリが接続可能で、前記不揮発性メモリを制御する制御プログラムをダウンロードするブートプログラムが格納された半導体集積回路装置であって、
前記ブートプログラムが格納されたブートプログラム格納用メモリと、
前記制御プログラムを格納する揮発性メモリと、
前記ブートプログラムに基づいて、前記制御プログラムのダウンロード、および前記制御プログラムに基づく前記不揮発性メモリの動作制御を行う制御部とを備え、
前記制御部は、ブートモードによる起動時において、プロテクトデータに応じて第１、または第２の状態のいずれであるかを判断し、前記第１の状態の際には、前記制御プログラムのダウンロードを実行し、前記第２の状態の際には、前記制御プログラムのダウンロードを実行しないことを特徴とする半導体集積回路装置。
【請求項3】
外付けで不揮発性メモリが接続可能で、前記不揮発性メモリを制御する制御プログラムをダウンロードするブートプログラムが格納された半導体集積回路装置であって、
前記ブートプログラム、および前記不揮発性メモリに格納されたユーザデータの読み出し動作を制御する通常動作用制御プログラムをダウンロードする通常動作用ブートプログラムがそれぞれ格納されたブートプログラム格納用メモリと、
前記制御プログラム、または通常動作用制御プログラムを格納する揮発性メモリと、
前記ブートプログラムに基づく前記制御プログラムのダウンロード、前記通常動作用ブートプログラムに基づく前記通常動作用制御プログラムのダウンロード、および前記制御プログラム、または前記通常動作用制御プログラムのいずれかに基づく前記不揮発性メモリの動作制御を行う制御部とを備え、
前記制御部は、ブートモードによる起動時において、プロテクトデータに応じて第１、または第２の状態のいずれであるかを判断し、前記第１の状態の際には、前記制御プログラムのダウンロードを実行し、前記第２の状態の際には、前記制御プログラムのダウンロードを実行しないことを特徴とする半導体集積回路装置。
【請求項4】
請求項１～３のいずれか１項に記載の半導体集積回路装置において、前記制御部は、前記制御プログラムをダウンロードする前に、前記プロテクトデータを読み出し、第１、または第２の状態のいずれであるかを判断することを特徴とする半導体集積回路装置。
【請求項5】
請求項４記載の半導体集積回路装置において、前記制御部は、前記第１の状態によって前記制御プログラムのダウンロードを実行した際に、前記不揮発性メモリのデータ領域に前記第２の状態となるプロテクトデータに書き換えることを特徴とする半導体集積回路装置。
【請求項6】
請求項１～５のいずれか１項に記載の半導体集積回路装置において、初期化終了後に、前記ブートモードを設定するブートモード設定用外部端子を有することを特徴とする半導体集積回路装置。

【請求項7】
ユーザデータが格納される不揮発性メモリと前記不揮発性メモリが外付けで接続可能な半導体集積回路装置とを有するデータ処理装置と、前記データ処理装置を管理する情報処理装置とよりなるデータ処理システムであって、
前記半導体集積回路装置は、
前記不揮発性メモリを制御する制御プログラムをダウンロードするブートプログラムが格納されたブートプログラム格納用メモリと、
前記制御プログラムを格納する揮発性メモリと、
前記ブートプログラムに基づいて、前記制御プログラムのダウンロード、および前記制御プログラムに基づく前記不揮発性メモリの動作制御を行う制御部とを備え、
前記不揮発性メモリは、第１、または第２の状態のいずれかの状態を設定するプロテクトデータが格納されるデータ領域を有し、
前記制御部は、ブートモードによる起動時において、前記不揮発性メモリのデータ領域に格納されたプロテクトデータを読み出し、第１、または第２の状態のいずれであるかを判断し、前記第１の状態の際には、前記情報処理装置からの前記制御プログラムのダウンロードを実行し、前記第２の状態の際には、前記制御プログラムのダウンロードを実行しないことを特徴とするデータ処理システム。
【請求項8】
ユーザデータが格納される不揮発性メモリと前記不揮発性メモリが外付けで接続可能な半導体集積回路装置とを有するデータ処理装置と、前記データ処理装置を管理する情報処理装置とよりなるデータ処理システムであって、
前記半導体集積回路装置は、
前記不揮発性メモリを制御する制御プログラムをダウンロードするブートプログラム、および前記不揮発性メモリに格納されたユーザデータの読み出し動作を制御する通常動作用制御プログラムをダウンロードする通常動作用ブートプログラムがそれぞれ格納されたブートプログラム格納用メモリと、
前記制御プログラム、または前記通常動作用制御プログラムを格納する揮発性メモリと、
前記ブートプログラムに基づく前記制御プログラムのダウンロード、前記通常動作用ブートプログラムに基づく前記通常動作用制御プログラムのダウンロード、および前記制御プログラム、または前記通常動作用制御プログラムのいずれかに基づく前記不揮発性メモリの動作制御を行う制御部とを備え、
前記制御部は、ブートモードによる起動時において、前記不揮発性メモリに格納されたプロテクトデータに応じて第１、または第２の状態のいずれであるかを判断し、前記第１の状態の際には、前記制御プログラムのダウンロードを実行し、前記第２の状態の際には、前記制御プログラムのダウンロードを実行しないことを特徴とするデータ処理システム。
【請求項9】
請求項７または８記載のデータ処理システムにおいて、前記制御部は、前記第１の状態により、前記情報処理装置からの前記制御プログラムのダウンロードを実行した際に、前記不揮発性メモリのデータ領域に前記第２の状態となるプロテクトデータに書き換えることを特徴とするデータ処理システム。
【請求項10】
請求項７～９のいずれか１項に記載のデータ処理システムにおいて、前記制御部は、前記制御プログラムを前記情報処理装置からダウンロードする前に、前記プロテクトデータを読み出し、第１、または第２の状態のいずれであるかを判断することを特徴とするデータ処理システム。
【請求項11】
請求項７～１０のいずれか１項に記載のデータ処理システムにおいて、前記半導体集積回路装置は、初期化終了後に、前記ブートモードを設定するブートモード設定用外部端子を有することを特徴とするデータ処理システム。

【発明の詳細な説明】

【０００１】
【発明の属する技術分野】
本発明は、データのプロテクト技術に関し、特に、ブートプログラムを備えた半導体集積回路装置におけるデータプロテクトに適用して有効な技術に関するものである。
【０００２】
【従来の技術】
フラッシュメモリなどの不揮発性メモリが備えられていない、いわゆる、ＲＯＭ（Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ）レスマイクロコンピュータなどの半導体集積回路装置をデータ処理システムなどに実装する際には、該ＲＯＭレスマイクロコンピュータとともにフラッシュメモリをプリント配線基板などの実装基板に実装する場合がある。
【０００３】
このＲＯＭレスマイクロコンピュータには、ブートプログラムが格納されている。このブートプログラムは、フラッシュメモリにアプリケーションプログラムなどのユーザデータを書き込むための書き込み制御プログラムをダウンロードするプログラムである。
【０００４】
そして、ＲＯＭレスマイクロコンピュータは、ブートプログラムによりダウンロードした書き込み制御プログラムに基づいて、フラッシュメモリにユーザデータを書き込む。
【０００５】
【発明が解決しようとする課題】
ところが、上記のような半導体集積回路装置におけるアプリケーションプログラムの書き込み技術では、次のような問題点があることが本発明者により見い出された。
【０００６】
フラッシュメモリに書き込まれたユーザデータは、ＲＯＭレスマイクロコンピュータからのアクセスが可能であるが、該ユーザデータにフラッシュメモリの読み出し機能がなければ、該フラッシュメモリが実装基板に実装されている限り、第三者がユーザデータを読み出すことはできない。
【０００７】
しかし、ＲＯＭレスマイクロコンピュータに格納されているブートプログラムを用いて、第三者が、書き込み制御プログラムの代わりに、フラッシュメモリの読み出し制御プログラムをダウンロードした場合、該ＲＯＭレスマイクロコンピュータを介して、フラッシュメモリに書き込まれたアプリケーションプログラムの内容が読み出されてしまう恐れがある。
【０００８】
本発明の目的は、ユーザデータの書き込み後に、該ユーザデータの読み出しを防止するプロテクトをかけることにより、ユーザデータの漏洩を防止することのできる半導体集積回路装置およびデータ処理システムを提供することにある。
【０００９】
本発明の前記ならびにその他の目的と新規な特徴は、本明細書の記述および添付図面から明らかになるであろう。
【００１０】
【課題を解決するための手段】
本願において開示される発明のうち、代表的なものの概要を簡単に説明すれば、以下のとおりである。
【００１１】
すなわち、本発明は、外付けでデータ書き換えが可能な不揮発性メモリが接続可能で、該不揮発性メモリを制御する制御プログラムをダウンロードするブートプログラムが格納された半導体集積回路装置であって、ブートプログラムに基づいて、制御プログラムをダウンロードする制御部を備え、該制御部は、ブートモードにおいて、プロテクトデータに応じて第１、または第２の状態のいずれであるかを判断し、第１の状態の際には制御プログラムのダウンロードを実行し、第２の状態では制御プログラムのダウンロードを実行しな

いものである。
【００１２】
また、本願のその他の発明の概要を簡単に示す。
【００１３】
また、本発明は、外付けで不揮発性メモリが接続可能で、該不揮発性メモリを制御する制御プログラムをダウンロードするブートプログラムが格納された半導体集積回路装置であって、ブートプログラムが格納されたブートプログラム格納用メモリと、制御プログラムを格納する揮発性メモリと、ブートプログラムに基づいて、制御プログラムのダウンロード、および制御プログラムに基づく不揮発性メモリの動作制御を行う制御部とを備え、制御部は、ブートモード時に、プロテクトデータに応じて第１、または第２の状態のいずれであるかを判断し、第１の状態の際には制御プログラムのダウンロードを実行し、第２の状態では、制御プログラムのダウンロードを実行しないものである。
【００１４】
さらに、本発明は、外付けで不揮発性メモリが接続可能で、該不揮発性メモリを制御する制御プログラムをダウンロードするブートプログラムが格納された半導体集積回路装置であって、ブートプログラム、および不揮発性メモリに格納されたユーザデータの読み出し動作を制御する通常動作用制御プログラムをダウンロードする通常動作用ブートプログラムがそれぞれ格納されたブートプログラム格納用メモリと、制御プログラム、または通常動作用制御プログラムを格納する揮発性メモリと、ブートプログラムに基づく制御プログラムのダウンロード、通常動作用ブートプログラムに基づく通常動作用制御プログラムのダウンロード、および制御プログラム、または通常動作用制御プログラムのいずれかに基づく不揮発性メモリの動作制御を行う制御部とを備え、制御部は、ブートモードによる起動時において、不揮発性メモリに格納されたプロテクトデータに応じて第１、または第２の状態のいずれであるかを判断し、第１の状態の際には制御プログラムのダウンロードを実行し、第２の状態の際では制御プログラムのダウンロードを実行しないものである。
【００１５】
ここで通常動作とは、該不揮発性メモリに格納される通常動作用ブートプログラム、通常動作用制御プログラム、ユーザーアプリケーションプログラム等のプログラムを実行する動作であり、半導体集積回路装置のリセット解除後、該通常動作用ブートプログラムから実行がなされるものである。
【００１６】
また、本発明は、ユーザデータが格納される不揮発性メモリと不揮発性メモリが外付けで接続可能な半導体集積回路装置とを有するデータ処理装置と、データ処理装置を管理する情報処理装置とよりなるデータ処理システムであって、半導体集積回路装置は、不揮発性メモリを制御する制御プログラムをダウンロードするブートプログラムが格納されたブートプログラム格納用メモリと、制御プログラムを格納する揮発性メモリと、ブートプログラムに基づいて、制御プログラムのダウンロード、および制御プログラムに基づく不揮発性メモリの動作制御を行う制御部とを備え、不揮発性メモリは、第１、または第２の状態のいずれかの状態を設定するプロテクトデータが格納されるデータ領域を有し、制御部は、ブートモードによる起動時において、不揮発性メモリのデータ領域に格納されたプロテクトデータを読み出し、第１、または第２の状態のいずれであるかを判断し、第１の状態の際には情報処理装置からの制御プログラムのダウンロードを実行し、第２の状態の際には制御プログラムのダウンロードを実行しないものである。
【００１７】
さらに、本発明は、ユーザデータが格納される不揮発性メモリと該不揮発性メモリが外付けで接続可能な半導体集積回路装置とを有するデータ処理装置と、該データ処理装置を管理する情報処理装置とよりなるデータ処理システムであって、半導体集積回路装置は、不揮発性メモリを制御する制御プログラムをダウンロードするブートプログラム、および不揮発性メモリに格納されたユーザデータの読み出し動作を制御する通常動作用制御プログラムをダウンロードする通常動作用ブートプログラムがそれぞれ格納されたブートプログ

ラム格納用メモリと、制御プログラム、または通常動作用制御プログラムを格納する揮発性メモリと、ブートプログラムに基づく制御プログラムのダウンロード、通常動作用ブートプログラムに基づく通常動作用制御プログラムのダウンロード、および制御プログラム、または通常動作用制御プログラムのいずれかに基づく不揮発性メモリの動作制御を行う制御部とを備え、制御部は、ブートモードによる起動時において、プロテクトデータに応じて第１、または第２の状態のいずれであるかを判断し、第１の状態の際には制御プログラムのダウンロードを実行し、第２の状態の際には制御プログラムのダウンロードを実行しないものである。

【００１８】

【発明の実施の形態】

以下、本発明の実施の形態を図面に基づいて詳細に説明する。

【００１９】

図１は、本発明の一実施の形態による半導体集積回路装置のブロック図、図２は、図１の半導体集積回路装置を用いて構成したデータ処理システムのブロック図、図３は、図２の半導体集積回路装置の各動作モードに対応するフラッシュメモリの状態説明図、図４は、図２のデータ処理システムにおける動作フローチャート、図５は、図１の半導体集積回路装置における状態遷移図、図６は、図１の半導体集積回路装置における端子機能の説明図、図７は、図２のデータ処理システムにおける通信動作処理の流れを示す説明図である。

【００２０】

本実施の形態において、半導体集積回路装置１は、たとえば、ＣＤ（Ｃｏｍｐａｃｔ　Ｄｉｓｃ）やＤＶＤ（Ｄｉｇｉｔａｌ　Ｖｅｒｓａｔｉｌｅ　Ｄｉｓｃ）などの光ディスク媒体に記憶されている情報の再生などを行うディスクドライブ装置に設けられ、光ディスク媒体のドライブ制御などを行う。

【００２１】

この半導体集積回路装置１は、フラッシュメモリなどの不揮発性メモリが内蔵されていない、いわゆる、ＲＯＭレスマイクロコンピュータからなる。この半導体集積回路装置１には、フラッシュメモリ（不揮発性メモリ）２（図２）が外部接続されている。

【００２２】

半導体集積回路装置１は、図１に示すように、中央処理装置（ＣＰＵ：Ｃｅｎｔａｒｌ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）３、ＲＡＭ（Ｒａｎｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙ）４、データ転送ユニット５、割り込みコントローラ６、ＢＳＣ（Ｂｕｓ　Ｓｔａｔｅ　Ｃｏｎｔｒｏｌｌｅｒ）７、周辺回路８、クロック発振器９、ブートＲＯＭ（Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ）１０、およびＩ／Ｏ（Ｉｎｐｕｔ／Ｏｕｔｐｕｔ）ポートＰなどから構成されている。

【００２３】

ＣＰＵ（制御部）３は、外部からの所定の信号などによってフラッシュメモリ２に格納された情報を読み出し、所定の処理を行う。また、ＣＰＵ３が処理を行うことによって生じたデータであって、半導体集積回路装置１に供給される電源が一時的に停止した後においても記憶しておくことが必要なデータはフラッシュメモリ２に書き込みがされる。

【００２４】

ＲＡＭ（揮発性メモリ）４は、随時読み出し／書き込みが可能なメモリであり、入出力データや演算データなどのＣＰＵ３などで利用されるユーザデータを一時的に格納する。データ転送ユニット５は、周辺回路８における各レジスタやＩ／ＯポートＰなどのデータ設定などを行う。

【００２５】

割り込みコントローラ６は、ＣＰＵ３やその他の周辺回路８などからの割り込み処理の制御を行う。ＢＳＣ７は、アドレス空間の分割、各種メモリ、周辺デバイスに応じた制御信号の出力を行う。

【００２６】

周辺回路８は、たとえば、ＷＤＴ（Ｗａｔｃｈ　Ｄｏｇ　Ｔｉｍｅｒ）１１、タイマ１２

、ＴＰＵ（Ｔｉｍｅｒ　Ｐｕｌｓｅ　Ｕｎｉｔ）１３、ＰＰＧ（Ｐｒｏｇｒａｍｍａｂｌｅ　Ｐｕｌｓｅ　Ｇｅｎｅｒａｔｏｒ）１４、ＳＣＩ（Ｓｅｒｉａｌ　Ｃｏｍｍｕｎｉｃａｔｉｏｎ　Ｉｎｔｅｒｆａｃｅ）１５、Ａ／Ｄ（Ａｎａｌｏｇ／Ｄｉｇｉｔａｌ）変換器１６、およびＤ／Ａ（Ｄｉｇｉｔａｌ／Ａｎａｌｏｇ）変換器１７などから構成されている。

【００２７】

ＷＤＴ１１は、半導体集積回路装置１の暴走などの監視を行う。タイマ１２は、たとえば、８ビットのカウンタをベースとしたタイマである。ＴＰＵ１３は、ＰＷＭ（Ｐｕｌｓｅ　Ｗｉｄｔｈ　Ｍｏｄｕｌａｔｉｏｎ）波形を出力することのできるタイマである。

【００２８】

ＰＰＧ１４は、任意の周期およびパルス幅のパルス出力波形を発生させる。ＳＣＩ１５は、外部接続されるデバイスとシリアル通信を行うインタフェースである。Ａ／Ｄ変換器１６は、アナログ信号をデジタル信号に変換して出力する。Ｄ／Ａ変換器１７は、デジタル信号をアナログ信号に変換して出力する。

【００２９】

クロック発振器９は、半導体集積回路装置１の動作の基本となるクロック信号を生成し、ＣＰＵ３、ＲＡＭ４、データ転送ユニット５、割り込みコントローラ６、ＢＳＣ７、ならびに周辺回路８にそれぞれ供給する。

【００３０】

ブートＲＯＭ（ブートプログラム格納用メモリ）１０は、フラッシュメモリを制御する制御プログラムをダウンロードするブートプログラムが格納される。ここでは、ダウンロードされる制御プログラムが、たとえば、フラッシュメモリ２への書き込み／消去動作を制御するプログラムとするが、該制御プログラムは、フラッシュメモリ２への書き込み／消去動作を制御するだけでなく、フラッシュメモリ２からの読み出し動作やその他の動作などを制御する機能を有するものであってもよい。

【００３１】

Ｉ／ＯポートＰは、データや制御信号などが入出力される外部ポートである。

【００３２】

ＣＰＵ３、ＲＡＭ４、データ転送ユニット５、ＢＳＣ７、およびブートＲＯＭ１０は、内部バスＢ１を介して相互に接続されている。ＢＳＣ７、および所定のＩ／ＯポートＰは、外部バスＢ２を介して相互に接続されている。割り込みコントローラ６、ＢＳＣ７、周辺回路８、ならびに所定のＩ／ＯポートＰは、周辺バスＢ３を介して相互にそれぞれ接続されている。

【００３３】

また、図２は、半導体集積回路装置１を用いてデータ処理システム１８を構成した一例を示す構成図である。データ処理システム１８は、パーソナルコンピュータなどのホスト（情報処理装置）Ｈ、および該ホストＨに接続されたディスクドライブ装置（データ処理装置）ＤＳなどから構成されている。

【００３４】

ホストＨとディスクドライブ装置ＤＳは、たとえば、ＡＴＡＰＩ（Ａｄｖａｎｃｅｄ　Ｔｅｃｈｎｏｌｏｇｙ　Ａｔｔａｃｈｍｅｎｔ　Ｐａｃｋｅｔ　Ｉｎｔｅｒｆａｃｅ）バスを介して双方向に信号伝送可能に接続されている。

【００３５】

ディスクドライブ装置ＤＳは、たとえば、ＣＤやＤＶＤなどの光ディスク媒体に記憶されている情報の再生などを行う。このディスクドライブ装置ＤＳには、光ディスク媒体のドライブ制御などを行う半導体集積回路装置１、およびフラッシュメモリ２が備えられている。

【００３６】

フラッシュメモリ２は、たとえば、アプリケーションプログラムなどのユーザデータが格納される記憶エリアＤＲ、およびプロテクトエリア（データ領域）ＰＲなどを有しており

、半導体集積回路装置１は、該フラッシュメモリ２に格納されたアプリケーションプログラムに基づいて光ディスク媒体のドライブ制御を行う。

【００３７】

また、プロテクトエリアＰＲは、半導体集積回路装置１がフラッシュメモリ２を制御する制御プログラムの転送を中止させるか、否か（若しくは許可させるか）を設定するプロテクトデータが格納される領域である。

【００３８】

図３は、半導体集積回路装置１の各動作モードにおけるフラッシュメモリ２の対応を示した図である。

【００３９】

図３においては、左側から右側にかけて、動作モード、フラッシュメモリ２のプロテクトエリアＰＲに格納されたプロテクトデータの値、データバス幅、起動エリア、および制御プログラムダウンロードの可／不可についてそれぞれ示している。

【００４０】

図示するように、たとえば、動作モードがブートモードの際には、データバス幅は８ビットとなり、起動はブートプログラムからとなる。このとき、フラッシュメモリ２のプロテクトエリアＰＲに「ＡＬＬ　Ｈ’ＦＦ」（たとえば、プロテクトエリアＰＲの全エリアに’１’のデータが格納されている状態）のプロテクトデータが格納されている場合、制御プログラムのダウンロードは可能（第１の状態）となる。

【００４１】

また、プロテクトエリアＰＲに「ＡＬＬ　Ｈ’ＦＦ」以外のプロテクトデータが格納されている場合、制御プログラムのダウンロードは不可（第２の状態）となる。プロテクトエリアＰＲのプロテクトデータが「ＡＬＬ　Ｈ’ＦＦ」、または「ＡＬＬ　Ｈ’ＦＦ」以外のいずれでもない場合には不定となり、フラッシュメモリ２の接続（データバス幅）により異なることになる。

【００４２】

次に、本実施の形態における半導体集積回路装置を用いたデータ処理システム１８の作用について説明する。

【００４３】

始めに、ホストＨからアプリケーションプログラムなどのユーザデータをフラッシュメモリ２に書き込み、プロテクトデータを設定するまでの動作について、図２、および図４のフローチャートを用いて説明する。

【００４４】

ここで、図２においては、動作処理に係わる主要なブロックのみを示しており、図２中に示した▲１▼～▲５▼、および▲１▼’は、動作の流れを示した番号である。

【００４５】

まず、リセットが解除され、半導体集積回路装置１がブートモードに遷移し（ステップＳ１０１）、ＣＰＵ３は、ブートＲＯＭ１０からフラッシュメモリ２の制御プログラムをダウンロードするためのブートプログラムを読み出す（▲１▼）。

【００４６】

ここで、図５は、半導体集積回路装置１における状態遷移を示す状態遷移図であり、図６は、半導体集積回路装置１の各ポート機能の説明図である。

【００４７】

図示するように、半導体集積回路装置１には、リセット端子ＲＥＳと、通常動作モード、またはブートモードモードを設定するモード端子（ブートモード設定用外部端子）ＭＤ０～ＭＤ２とが設けられている。

【００４８】

たとえば、リセット端子ＲＥＳに’０’（Ｌｏ信号）が入力された際には半導体集積回路装置１がリセット状態となり（状態Ｊ１）、モード端子ＭＤ１に’０’、モード端子ＭＤ２に’１’（Ｈｉ信号）が入力された際には該半導体集積回路装置１が通常動作モードと

なる（状態Ｊ２）。

【００４９】

また、モード端子ＭＤ２，０に’０’、モード端子ＭＤ１に’１’が入力されると、半導体集積回路装置１はブートモードに遷移する（状態Ｊ３）。

【００５０】

続いて、図２、図４に示すように、ホストＨとのビットレートの合わせ込みを行った後（ステップＳ１０２）、ＣＰＵ３は、フラッシュメモリ２のプロテクトエリアＰＲに書き込まれているプロテクトデータを参照し（▲１▼’）、該プロテクトデータがプロテクト状態となっているか、否かを判断する（ステップＳ１０３）。

【００５１】

このとき、プロテクトデータがプロテクト状態（第２の状態）となっている際には、半導体集積回路装置１は、スタンバイ状態（あるいは、スリープ状態、無限ループ）となる（ステップＳ１０４）。

【００５２】

ステップＳ１０３の処理において、フラッシュメモリ２のプロテクトデータがプロテクト状態となっていない場合（第１の状態）には、ＣＰＵ３は、ブートプログラムに基づいて、フラッシュメモリ２の制御プログラム（▲２▼）をホストＨからＳＣＩ１５を介してＲＡＭ４にダウンロードする（ステップＳ１０５）。

【００５３】

そして、ＣＰＵ３は、ＲＡＭ４にダウンロードされた制御プログラムに基づいて（ステップＳ１０６）、フラッシュメモリ２の書き込み／消去動作を制御する（▲３▼）。

【００５４】

そして、ホストからデータ書き込み、あるいはデータ消去のコマンドを受信すると（ステップＳ１０７）、半導体集積回路装置１は、フラッシュメモリ２のデータ消去（ステップＳ１０８）、または該コマンドに従ってフラッシュメモリ２へのデータ書き込み（ステップＳ１０９）を行う。

【００５５】

たとえば、ステップＳ１０７の処理において、アプリケーションプログラムなどのユーザデータをフラッシュメモリ２に書き込む際には、ホストＨから半導体集積回路装置１にデータ書き込みのコマンドが出力される。

【００５６】

このコマンドを受け取ると、ホストＨからユーザデータ（▲４▼）が半導体集積回路装置１に出力され、ＳＣＩ１５を介してＲＡＭ４にダウンロードされる。そして、ＣＰＵ３は、制御プログラムに基づいて、ＲＡＭ４にダウンロードされたユーザデータをフラッシュメモリ２の記憶エリアＤＲに書き込む（▲５▼）。このとき、ＣＰＵ３は、フラッシュメモリ２のプロテクトエリアＰＲに、「Ｈ’ＦＦ」以外の任意の値をプロテクトデータとして書き込む。

【００５７】

次回からは、半導体集積回路装置１がブートモードによって起動しても、ステップＳ１０３の処理において、プロテクトデータがプロテクト状態となっていると判断するので、半導体集積回路装置１がスタンバイ状態となり、制御プログラムのダウンロードが一切行われないことになる。

【００５８】

これにより、フラッシュメモリ２に格納されたユーザデータの再書き込みや消去などが防止されるだけでなく、たとえば、読み出し動作を制御する制御プログラムなどのダウンロードも防止することができるので、第三者などによるユーザデータの読み出しなども防止することができる。

【００５９】

また、ブートモード起動時の半導体集積回路装置１とホストＨとの通信プロトコルについて、図７を用いて説明する。

【００６０】
図７においては、上方から下方にかけて、ビットレートの合わせ込み時、制御プログラムの転送時、および制御プログラムの実行時における半導体集積回路装置１、およびホストＨの処理動作の流れについてそれぞれ示している。
【００６１】
まず、ビットレートの合わせ込みを行う場合、ホストＨは、所定のビットレートでデータ「Ｈ’００」を半導体集積回路装置１に連続送信する。半導体集積回路装置１は、受信した「Ｈ’００」のＬｏｗレベル期間を測定してビットレートを計算し、たとえばＲＳ－２３２調歩同期シリアル通信のビットレートを設定する。
【００６２】
ここで、ホストＨと半導体集積回路装置１との通信は、ＲＳ－２３２調歩同期シリアル通信以外でもよく、たとえば、ＵＳＢやイーサネット（登録商標）などを用いて通信することにより、より高速なデータ転送を可能とすることができる。
【００６３】
その後、半導体集積回路装置１は、ビットレートの設定終了の合図として「Ｈ’００」などの１バイトデータをホストＨに送信する。ホストＨは、「Ｈ’００」を受信すると、たとえば、「Ｈ’５５」などの１バイトデータを半導体集積回路装置１に送信する。
【００６４】
半導体集積回路装置１は、「Ｈ’５５」のデータを受け取ると、フラッシュメモリ２のプロテクトエリアＰＲに記憶されているプロテクトデータを読み出し、該プロテクトデータが「Ｈ’ＦＦ」であれば、制御プログラムのダウンロードが可能であることを示す「Ｈ’ＡＡ」などのデータをホストＨに送信する。
【００６５】
また、半導体集積回路装置１は、プロテクトデータが「Ｈ’ＦＦ」以外であれば、制御プログラムのダウンロードが不可であることを示す「Ｈ’ＦＦ」のデータをホストＨに送信し、動作を停止（スタンバイ状態など）する。
【００６６】
次に、制御プログラムの転送時において、ホストＨは、転送する制御プログラムのバイト数（Ｎ）を上位バイト、下位バイトの順に２バイト送信する。そして、半導体集積回路装置１は、受信した２バイトデータをエコーバックする。
【００６７】
その後、ホストＨは、制御プログラムを１バイト毎に送信する（Ｎ回繰り返し）。半導体集積回路装置１は、受信したデータをホストＨにエコーバックするとともに、ＲＡＭ４に転送する（Ｎ回繰り返し）。そして、すべてのデータの受信が完了すると、半導体集積回路装置１は、「Ｈ’ＡＡ」をホストＨに送信する。
【００６８】
続いて、制御プログラムの実行において、半導体集積回路装置１は、ＲＡＭ４に格納された制御プログラムに基づいてフラッシュメモリ２の書き込み／消去動作の制御を行う。
【００６９】
それにより、本実施の形態においては、フラッシュメモリ２へのユーザデータの書き込み後にプロテクトデータによってプロテクトをかけることにより、半導体集積回路装置１を用いた該フラッシュメモリ２へのユーザデータの再書き込み／消去／読み出しなどを防止することができる。
【００７０】
また、本実施の形態においては、プロテクトデータの判断（図４、ステップＳ１０３）をビットレートの合わせ込みが終了した後に行っていたが、このプロテクトデータの判断はこれに限定されるものではない。
【００７１】
たとえば、ビットレートの合わせ込み（図４、ステップＳ１０２）の前や、制御プログラムをＲＡＭ４にダウンロード（図４、ステップＳ１０５）した後など、プロテクトデータ

の判断は、制御プログラムによるフラッシュメモリ２の制御が行われる以前であれば、どのようなタイミングであってもよい。

【００７２】

以上、本発明者によってなされた発明を発明の実施の形態に基づき具体的に説明したが、本発明は前記実施の形態に限定されるものではなく、その要旨を逸脱しない範囲で種々変更可能であることはいうまでもない。

【００７３】

【発明の効果】

本願によって開示される発明のうち、代表的なものによって得られる効果を簡単に説明すれば、以下のとおりである。

【００７４】

（１）不揮発性メモリへのユーザデータの書き込み後に第２の状態となるプロテクトデータを設定することにより、半導体集積回路装置を用いての該不揮発性メモリへのユーザデータの再書き込み／消去／読み出しなどを確実に防止することができる。

【００７５】

（２）上記（１）により、不揮発性メモリを取り外さない限り、該不揮発性メモリに格納されたユーザデータを隠蔽できるので、データ処理システムの信頼性を大幅に向上することができる。

【図面の簡単な説明】

【図１】本発明の一実施の形態による半導体集積回路装置のブロック図である。

【図２】図１の半導体集積回路装置を用いて構成したデータ処理システムのブロック図である。

【図３】図２の半導体集積回路装置の各動作モードに対応するフラッシュメモリの状態説明図である。

【図４】図２のデータ処理システムにおける動作フローチャートである。

【図５】図１の半導体集積回路装置における状態遷移図である。

【図６】図１の半導体集積回路装置における端子機能の説明図である。

【図７】図２のデータ処理システムにおける通信動作処理の流れを示す説明図である。

【符号の説明】

１　半導体集積回路装置
２　フラッシュメモリ（不揮発性メモリ）
３　ＣＰＵ（制御部）
４　ＲＡＭ（揮発性メモリ）
５　データ転送ユニット
６　割り込みコントローラ
７　ＢＳＣ
８　周辺回路
９　クロック発振器
１０　ブートＲＯＭ（ブートプログラム格納用メモリ）
１１　ＷＤＴ
１２　タイマ
１３　ＴＰＵ
１４　ＰＰＧ
１５　ＳＣＩ
１６　Ａ／Ｄ変換器
１７　Ｄ／Ａ変換器
１８　データ処理システム
Ｈ　ホスト（情報処理装置）
ＤＳ　ディスクドライブ装置（データ処理装置）
Ｐ　Ｉ／Ｏポート

ＭＤ０～ＭＤ２　モード端子（ブートモード設定用外部端子）
ＲＥＳ　リセット端子

【図1】

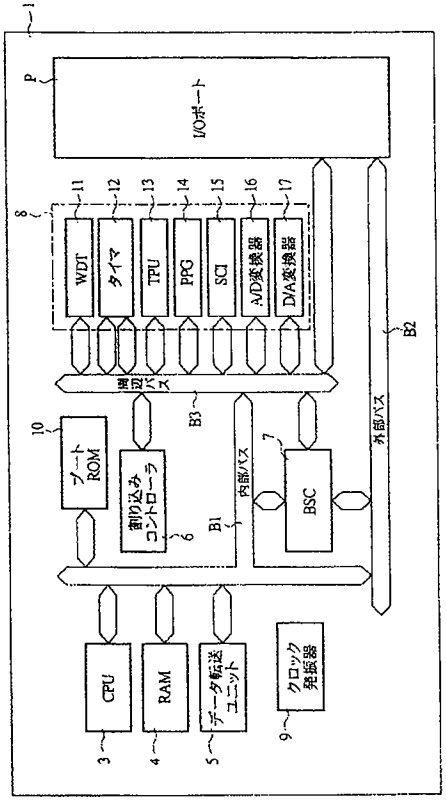


図 1

【図2】

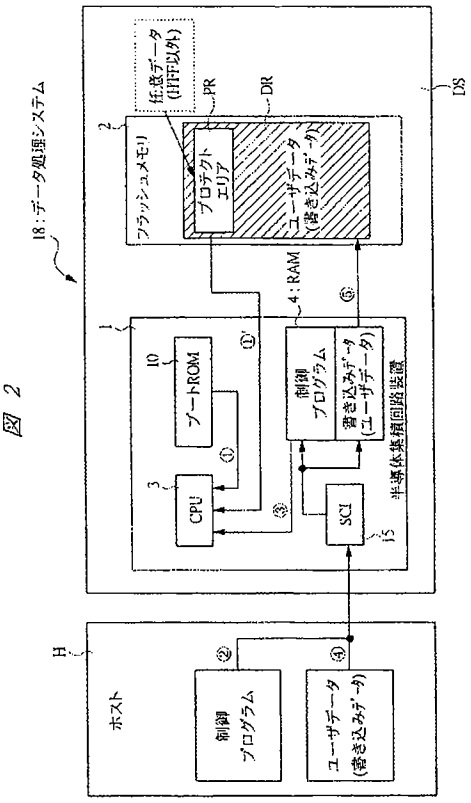


図 2

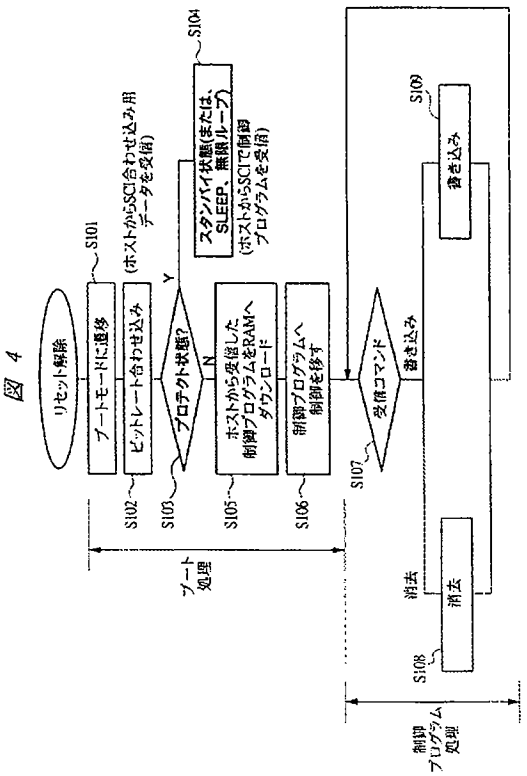
【図3】

図 3

No.	動作モード	フラッシュメモリ上のプロテクトエリアの値	データバス幅	起動エリア	制御プログラムダウンロードの可／不可
1	拡張モード1	—	8ビット	フラッシュメモリ（ユーザプログラム）	—
2	拡張モード2	—	16ビット	フラッシュメモリ（ユーザプログラム）	—
3	拡張モード3	—	32ビット	フラッシュメモリ（ユーザプログラム）	—
4	ブートモード	ALL H'FF	8ビット	ブートプログラム	可
5		ALL H'FF以外	8ビット	ブートプログラム	不可
6		ALL H'FFまたは、ALL H'FF以外でない	8ビット	ブートプログラム	不定（メモリの接続方法により異なる。）

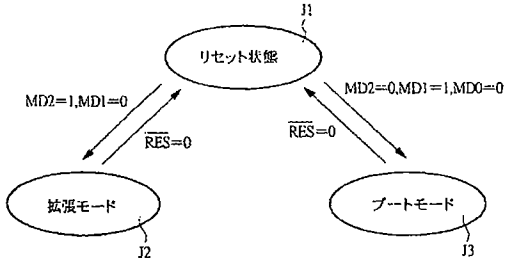
【図4】

図 4



【図5】

図 5



【図6】

図 6

端子名	入出力	機能
RES	入力	リセット
MD2	入力	動作モードを設定
MD1	入力	動作モードを設定
MD0	入力	動作モードを設定

【図7】

図 7

項目		ホストの動作	半導体集積回路装置の動作
ブートモード起動			リセットスタート後ブートプログラムへ分岐
ビットレート合わせ込み		所定のビットレートでデータH'00を連続送信	受信データH'00のLow期間を測定 ビットレートを計算し、RS-232Cシリアル通信を設定 ビットレート調整終了の合図としてH'00を1バイト送信
		H'00を正常に受信したらH'55を1バイト送信	H'55を受信
		H'AAを受信	フラッシュメモリ内のプロテクトエリアをリードするプロテクトコードが一致したらホストへH'AAを送信する(不一致の場合はH'FFを送信し動作を停止)
制御プログラムの転送		転送する制御プログラムのバイト数(N)を上位バイト、下位バイトの順に2バイト送信	受信した2バイトのデータをホストへエコーバック
		制御プログラムを1バイト毎に送信(N回繰り返し)	受信したデータをホストにエコーバックすると共にRAMへ転送する(N回繰り返し)
		H'AAを受信	受信完了の合図としてH'AAを送信
制御プログラムの実行			RAMに転送された制御プログラムへ分岐し実行を開始

PATENT ABSTRACTS OF JAPAN

(11)Publication number : **2004-318330**
(43)Date of publication of application : **11.11.2004**

(51)Int.Cl. G06F 11/00
G06F 1/00
G06F 9/445
G06F 12/14

(21)Application number : **2003-109170**
(22)Date of filing : **14.04.2003**

(71)Applicant : **RENESAS TECHNOLOGY CORP**
(72)Inventor : **IIJIMA MASAHITO**
ASAI TOSHIO

(54) SEMICONDUCTOR INTEGRATED CIRCUIT DEVICE AND DATA PROCESSING SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To prevent leakage of user data after writing them in a semiconductor integrated circuit device allowing connection of an external non-volatile memory.
SOLUTION: When the semiconductor integrated circuit device 1 is shifted to a boot mode after resetting, a CPU 3 reads a boot program for downloading a control program for a flash memory 2 from a boot ROM 10. Subsequently, matching of a bit rate with a host H is carried out, and the CPU 3 refers protect data written in a protect area PR of the flash memory 2 for determining whether the protect data are in a protected condition. In this process, if the protect data are in the protected condition, the semiconductor circuit device 1 is set to a standby condition (a sleep condition or an endless loop), and consequently, downloading of the control program cannot be executed at all.